Ministerstwo
Cyfryzacji

Centrum Certyfikacji
Ministerstwo Cyfryzacji

Specyfikacja tokenów dla SRP

1. Wspierane systemy operacyjne

Urządzenie musi zapewniać poprawną współpracę z systemami operacyjnymi:

- Linux (32/64 Bit),
- Windows 10,
- Windows 8,
- Windows 7 (32/64 Bit).

2. Wspierane API i standardy

Urządzenie musi wspierać i być zgodne z poniższym:

- PKCS#11 v2.01,
- Microsoft CAPI,
- PC/SC, X.509 v3 certificate storage,
- SSL v3,
- IPsec/IKE.

3. Wspierane oprogramowanie

Urządzenie musi być zgodne z oprogramowaniem:

- JAVA (1.6/1.7),
- Openssl (engine),
- PCSCD (Linux).

4. Wspierane algorytmy

Urządzenie musi wspierać algorytmy:

- RSA 1024/2048 bit,
- DES,
- 3DES,
- SHA1,
- SHA256,
- ECC p.256/p.384,
- AES 128/192/256 bit.

Zalecana obsługa algorytmów haszujących SHA-384 i SHA-512.

5. Certyfikaty bezpieczeństwa

Urządzenie musi posiadać certyfikat FIPS 140-2 level 3 (całość urządzenia) lub CC EAL5+.

6. Specyfikacja sprzętowa

Urządzenie musi poprawnie pracować w temperaturze 5°C do 40°C.

Interface USB typ A (USB 1.1 i 2.0).

7. Specyfikacja pamięci

Urządzenie musi zapewniać przechowywanie danych przez co najmniej 10 lat.

Ilość cykli zapisu nie może być mniejsza niż 500 000.

8. Wymagania bezpieczeństwa

Urządzenie musi uniemożliwiać eksport klucza prywatnego.

Urządzenie musi umożliwiać dostęp do klucza prywatnego po podaniu kodu PIN.